SAE ARP 4761: Excellence in Procedure for Safety Assessment

Berquó, Jolan Eduardo – Electronic Eng. (ITA)
Aerospace Product Certifier (DCTA/IFI)
Government Representative for Quality Assurance – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

IYK 37– JUN 04 2013

We will present in this MSC an analysis about the importance of the ARP 4761, a document developed by the Committee S-18, installed in the SAE Aerospace, a group of SAE International. This document was prepared for conducting Safety Assessment (Safety Assessment) for large civil aircraft, and considered by the FAA as an acceptable methodology to demonstrate compliance with the safety requirements of 14 CFR Part 25.1309 (FAR 25.1309). We will conclude this IYK with a challenge to safety analysts that read us.

We have already discussed a little the ARP 4761, in the MSC 09, 10 and 11, which deal with the Safety Assessment, a document that is related to ARP 4754 (Guidelines for Development of Civil Aircraft and Systems), but we did not go deeper on that occasion, that is, we did not discuss what would have led SAE to create the SAE S-18 to prepare the ARP 4761

We started, noting that the AC (Advisory Circular) 25-1309-1A, which, like all AC, was prepared as an attempt to help the applicant in assessing the safety, according to the requirements (b), (c) and (d) of FAR 25.1309, is not an easy document to understand in terms of logical sequencing of its process.

The AC is a very well intentioned document, but its paragraphs, in our opinion, are not conclusive by itself. It discuss, for example, a particular task, in a paragraph, relating it to several others, in other paragraphs, ahead or already addressed somewhere, bringing, in this coming and going, reasonable difficulty for the analyst.

Anyone wishing to summarize the AC, trying to make it more palatable, will have a formidable task ahead, something as to write a monograph. We know this because we already done it some time ago.

Therefore, we believe that it was no surprise the decision of SAE to organize a committee (S-18) to propose the methodology reported in ARP 4761. The logic of the process is crystalline, although it is somewhat complex, but solely and uniquely just because of the interminable iterations through the process. The document is in fact much more iterative than sequential.

But the idea contained in 4761 to develop the Safety Assessment through the FHA (Functional Hazard Assessment), initially applied to the functions of the aircraft, a "top-down" process, was simply brilliant. Incidentally, in this context, we paraphrase the great and beloved Brazilian teacher Francisco Antonio Lacaz Neto, who was rector of our *Instituto Tecnológico de Aeronáutica (ITA), in São José dos Campos (SP), Brazil*. He told us, on one occasion: "Great ideas are simple."

We believe that was really good having emerged AC 25.1309-1A, trying to help applicants for certification, because it led to the American Aviation Community, through SAE, to develop the process decidedly aimed at simplifying the suggestion contained on the mentioned AC. If it were simple, it would not be necessary to draw up the 4761.

The most interesting is that the idea contained in the ARP 4754 and 4761 was already latent in the Engineering and Systems Analysis (EAS). But the SAE, without escaping from the methodology of EAS, has introduced a process indeed clearer and simplifier.

As we have said, it is complex, but only by its intense iterative rhythm. But the important thing is the simplicity of the logic of proposed process, not leaving us pondering for long time, as we do when we decided to strictly follow the AC 25.1309-1A.

Let us go now interpret the reasoning of the ARP. "An aircraft is something that was made to fly. For doing this, it needs something called engine-propeller system. It would not raise flight if there were not something for it to go

ahead on a runway until it reaches a speed that allowed it to take off: the landing gear. Other fundamental things also to take off, to land and control flight attitudes are the so called flight control surfaces. On the other hand, to orient itself in the air, when flying, something else is needed to promote this guidance. And so it goes: things and things. But the most important thing is the fallible thing called pilot".

The fact is that everything has its function. Someone can identify a number of functions of the aircraft. Somel functions are absolutely critical if missing. Such functions are those whose absence can lead to catastrophic accidents. The lack of others functions in spite of not being catastrophic, can, however, lead to situations of much workload for the crew and discomfort for passengers, while the lack of others functions do not result in major consequences.

So, it seems easy to understand that we should start our safety evaluation, assessing the consequences of loss of aircraft functions. But it is not always trivial to identify all functions that must be present in an aircraft. This depends on the complexity of the aircraft. Can you imagine the amount of functions of an aircraft as the Boeing 787 or the Airbus 380?

This is the reason by what the ARP 4761, wisely, admits that the first identification of the functions of the aircraft should be regarded as preliminary. During the further development of the systems and their architecture, can arise more functions. Therein lies the reason for the intense interactivity of the ARP.

Well but the fact is that, once identified preliminarily the functions of the aircraft, the process continues with the allocation of safety requirements for each identified function. The requirements are derived from FAR 25.1309, already mentioned, requirements of potential customers and the company's own requirements.

It is notable the utilization of the technique of Fault Tree Analysis (FTA), in the allocation of safety requirements for aircraft functions, and then to the functions of the systems. Other techniques are suggested in 4761, but FTA is by far the most used. It is a type of analysis that uses the axioms and properties of the calculus of probabilities associated with the Boolean Algebra in his "Theory of Sets" of mathematics.

It is not difficult go from the functions of the aircraft to the functions of the systems required for carrying out the functions of the aircraft, and perform the respective allocations of safety requirements for such systems.

At this moment, as we said, there could be new functions for the aircraft or new functions for the systems. The reality is that the process is highly iterative, and more iterative than sequential.

Once defined the systems, with their allocated requirements, we go to the identification of items (mainly equipment) that will provide the systems' architecture. In this phase, the designers develop the interconnection of the items and the installation processes on the aircraft.

Conceptually, this is the process, but to develop it, as already mentioned, are considered other analysis techniques, in addition to the FTA

In fact, the great merit of 4761 is to provide a process that can be an excellent alternative to the AC-1A 25-1309 and has the consent of the Airworthiness Authority (FAA, EASA, ANAC). The process can also be applied to the demonstration of compliance with the requirements of the FAR 23.1309, taking into account only the observations of caution contained in AC 23.1309-1E.

But pay attention to the following: after the analyst becomes familiar with the 4761 and knows well the purpose of AC 25.1309-1A (or 23.1309-1E), he can establish its own procedure, based on the 4761. This is possible because, as mentioned on the AC mentioned, there is not only one way to demonstrate the compliance with the safety requirements of FAR 25.1309 and FAR 23.1309

By the way, we present now a great challenge for safety analysts: "Develop your own procedure for their companies, from the 4761, trying to reduce the intense interactivity contained in that document (this would be the big challenge). At least, you would have the opportunity to go deeper in the subject ".

We are developing a work of this nature, already at an advanced stage, from which we intend to develop a course. It's fascinating. Try to develop your own work, and we will discuss it together. But pay attention: it is necessary to have patience. We can do anything, provided we have dedication and patience.

Thank you very much. See you.

References:

(1) **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, USA, 1996.

(2) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, 2007.

(3) **FAA**: AC 25.1309-1A, System Design and Analysis, USA, 1988.

(4) **FAA**: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes, USA, 2011.